Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

01 November 2021

PIN Number

20211101-001

Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims

Summary

The FBI assesses ransomware actors are very likely using significant financial events, such as mergers and acquisitions, to target and leverage victim companies for ransomware infections. Prior to an attack, ransomware actors research publicly available information, such as a victim's stock valuation, as well as material nonpublic information. If victims do not pay a ransom quickly, ransomware actors will threaten to disclose this information publicly, causing potential investor backlash.

Threat

Ransomware actors are targeting companies involved in significant, time-sensitive financial events to incentivize ransom payment by these victims. Ransomware is often a two-stage process beginning with an initial intrusion through a trojan malware, which allows an access broker to perform reconnaissance and determine how to best monetize the access. However, while this malware is often mass distributed, most victims of trojans are not also victims of ransomware, indicating ransomware targets are often carefully selected from a pool based on information gleaned from the initial reconnaissance. During the initial reconnaissance phase, cyber criminals identify non-publicly available information, which they threaten to release or use as leverage during the extortion to entice victims to comply with ransom demands. Impending events that could affect a victim's stock value, such as announcements, mergers, and acquisitions, encourage ransomware actors to target a network or adjust their timeline for extortion where access is established.

- In early 2020, a ransomware actor using the moniker "Unknown" made a post on the Russian hacking forum "Exploit" that encouraged using the NASDAQ stock exchange to influence the extortion process. Following this posting, unidentified ransomware actors negotiating a payment with a victim during a March 2020 ransomware event stated, "We have also noticed that you have stocks. If you will not engage us for negotiation we will leak your data to the nasdaq and we will see what's gonna (sic) happen with your stocks."
- Between March and July 2020, at least three publicly traded US companies actively involved in mergers and acquisitions were victims of ransomware during their respective negotiations. Of the three pending mergers, two of the three were under private negotiations.
- A November 2020 technical analysis of Pyxie RAT, a remote access trojan that often precedes Defray777/RansomEXX ransomware infections, identified several keyword searches on a victim's network indicating an interest in the victim's current and near future stock share price. These keywords included 10-q[1], 10-sb[2], n-csr[3], nasdaq, marketwired, and newswire.

[1] 10-Q is a quarterly report that must be submitted by all publicly traded companies disclosing relevant information regarding finances.
[2] 10-SB was a filing form used to register the securities of small businesses who wished to trade on U.S. exchanges.
[3] N-CSR is a form that registered management investment companies must file with the Securities and Exchange Commission within 10 days after a company disseminates annual and semi-annual reports to stockholders.

- In April 2021, Darkside ransomware[4] actors posted a message on their blog site to show their interest in impacting a victim's share price. The message stated, "Now our team and partners encrypt many companies that are trading on NASDAQ and other stock exchanges. If the company refuses to pay, we are ready to provide information before the publication, so that it would be possible to earn in the reduction price of shares. Write to us in 'Contact Us' and we will provide you with detailed information."

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom emboldens adversaries to target additional organizations, encourages other criminal actors to engage in the distribution of ransomware, and/or may fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to your local FBI field office. Doing so provides the FBI with the critical information they need to prevent future attacks by identifying and tracking ransomware attackers and holding them accountable under US law.

Recommendations

- Back-up critical data offline.
- Ensure copies of critical data are in the cloud or on an external hard drive or storage device.
- Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the original data resides.
- Install and regularly update anti-virus or anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks.
- Use two-factor authentication for user login credentials, use authenticator apps rather than email as actors may be in control of victim email accounts and do not click on unsolicited attachments or links in emails.
- Implement least privilege for file, directory, and network share permissions.

[4] Darkside is a ransomware-as-a-service variant, in which criminal affiliates conduct the attacks and the proceeds are shared with the ransomware developer(s). Darkside ransomware was used in the May 2021 Colonial Pipeline intrusion.

- Review the following additional resources.
  - The joint advisory from Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious Activity provides additional guidance when hunting or investigating a network and common mistakes to avoid in incident handling.
  - The Cybersecurity and Infrastructure Security Agency-Multi-State Information Sharing & Analysis Center Joint Ransomware Guide covers additional best practices and ways to prevent, protect, and respond to a ransomware attack.
  - StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, the information in this product may be shared without restriction.

